AARP Public Policy Institute

FACT SHEET

GONE PHISHING: THE INTERNET AND IDENTITY THEFT

Phishing Defined

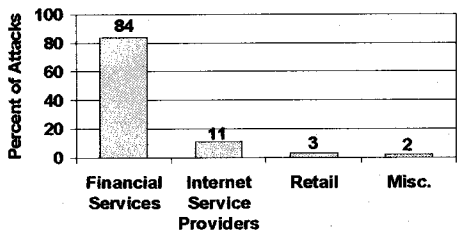
Phishing is a form of Internet fraud that involves sending an email message to an Internet user falsely claiming to represent a legitimate enterprise. This is done in an attempt to trick the user into visiting a fraudulent website and disclosing sensitive personal information that would then be used to commit identity theft. Phishing is a play on the word, "fishing," since the phisher is putting out bait in the hope that at least some people will be enticed to respond to the message.[1]

The Anti-Phishing Working Group (APWG), an industry-sponsored association, estimates that 75 million to 150 million phishing emails are sent daily.[2] Despite the fact that many of these messages are blocked by spam filters and never reach Internet users, it is estimated that a well-designed phishing email campaign can have response rates of up to 5 percent.[3]

Phishers often choose to target large financial institutions known to have a significant online customer base. This is done with the knowledge that a certain percentage of the email message recipients will be actual customers of the institution and likely to believe that the message is legitimate. Typically, the message attempts to spur the user to act before some adverse consequence occurs, such as having one's account cancelled or blocked.

Also targeted are websites belonging to Internet service providers, retailers, and even government agencies. Chart 1 illustrates the breakdown of industry sectors that were targeted most frequently by phishing attacks during April 2005.

Chart 1
Industry Sector Most Targeted by Phishing Attacks
April 2005



Prepared by AARP Public Policy Institute
Source: Anti-Phishing Working Group Phishing Activity Trend Report, June 2, 2005.

Once users have contacted the fraudulent website, they are asked to provide or update personal information, such as credit card or bank account number, account username, password, security code, Social Security number, or other sensitive personal information that is already held by the legitimate organization.

After collecting the information, the phisher will often sell the victim's personal information via the Internet to others who intend to use the information to commit fraud.[4] With their personal information compromised, the victim is at risk of a number of possible frauds:

- The information can be used to access existing financial accounts.
- The information can be used to apply for credit and open new accounts in the victim's name.
- The information can be used to hijack the victim's computer and use it as a platform to disseminate phishing and spam email messages to others.

The Increase in Phishing Attacks

Phishing frauds have become increasingly easy to perpetrate, with ready-made phishing toolkits and

---

[1] Another form of phishing, called "pharming," involves using computer program tricks to redirect Internet users from a legitimate site to a fraudulent site operated by criminals.

[2] APWG. "Commentary to FDIC 'Putting an End to Account-Hijacking Identity Theft,'" Feb. 4, 2005, http://www.antiphishing.org/APWG-FDICCommentaryLetter.doc.

[3] B. Sullivan. *Your Evil Twin: Behind the Identity Theft Epidemic*. John Wiley & Sons, Inc., 2004.

[4] Federal Deposit Insurance Corporation (FDIC). "*Putting an End to Account-Hijacking Identity Theft*," December 14, 2004, http://www.fdic.gov/consumers/consumer/idtheftstudy.